Journal of Cybersecurity Education, Research and Practice

Volume 2016
Number 2 *Two*

Article 4

December 2016

Threats to Information Protection - Industry and Academic Perspectives: An annotated bibliography

Michael E. Whitman
Kennesaw State University, mwhitman@kennesaw.edu

Herbert J. Mattord
Kennesaw State University, hmattord@kennesaw.edu

Threats to Information Protection - Industry and Academic Perspectives: An annotated bibliography

Abstract
Threats to information assets have always been a concern to those responsible for making information useful and defending its value. The concepts of threat, threat agent, threat events and threat sources have evolved in recent years have very precise definitions. A summary of threat classification models used in academic research is provided along with a summary of recent industry threat assessment reports. Finally, the results from a recent study, *2015 SEC/CISE Threats to Information Protection Report Including a Current Snapshot of the State of the Industry*, are given.

Keywords
information security, cybersecurity, threats, threat agents

Cover Page Footnote
An abstract and summary of an earlier version of this article was published in the proceedings of the 2016 Conference on Cybersecurity Education, Research, and Practice.

INTRODUCTION

Threats and the agencies that bring the risk of loss from them have always been present in the realm of information protection. Since the first records were kept, maintaining the availability and integrity of the information was a vital element of every record keeping technology, from cuneiform on clay tablets to today's digital records. The characteristic of confidentiality has been added to the essential list as information owners sought to preserve privacy and maintain secrecy. The importance of information protection comes to the fore as information owners and custodians strive to maintain the three primary characteristics of information which need protection – confidentiality, integrity and availability.

The purpose of this paper is to document the evolution and understanding of threats to information as a method of supporting academic research and instruction in cybersecurity. It will also serve as a summary of the current threat environment experienced in the area of information protection. Only by understanding its adversaries can an organization hope to protect its information assets. Given the complex and ever changing threat environment, defense from attack relies on persistence in devising and maintaining defenses against attacks on systems that store, process and transmit information and also requires constant vigilance and awareness of emerging and changing threats.

WHAT IS THE THREAT?

Industry and academic professionals alike will acknowledge a general understanding of the concept of a threat. Information security threats are modeled after physical threats (such as theft, trespassing, and fraud), as are the laws that govern computer crimes. In order to establish a common language for the purposes of this paper, the following descriptions of threats taken from a popular information security text will be employed:

> *Threat - Any event or circumstance that has the potential to adversely affect operations and assets. The term "threat source" is commonly used interchangeably with the more generic term "threat", however, threat is a much more amorphous manifestation of potential risk compared to the categorical definitions commonly used as threat sources.*
>
> *Threat agent - The specific instance or a component of a threat. For example, the threat source of "trespass or espionage" is a category of potential danger to information assets, while "external professional hacker" is a specific threat agent. A lightning strike, hailstorm, or tornado is a threat agent that is part of the threat source known as acts of God/acts of nature.*

Threat event - An occurrence of an event caused by a threat agent. An example of a threat event might be damage caused by a storm. This term is commonly used interchangeably with the term "attack".

Threat source - A categorization of objects, people, or other entities that represents the origin of danger to an asset. In other words, a categorization of threat agents. For example, acts of trespass or espionage or acts of God/acts of nature (Whitman & Mattord, 2016).

CLASSIFICATION MODELS OF THREATS

As is commonly done when attempting to understand a specific phenomenon, academics begin examining threats by creating classifications or categorization models. The following articles include the earliest and as well as some of the most recent threat classification models.

Loch, K. D., Carr, H. H., and Warkentin, M. E. (1992) Threats to information systems: Today's reality, yesterday's understanding. MISQ. 16(2), 173–186.

This article, which is discussed in more detail in the Academic Studies section later in this paper, initially proposed a four dimensional model of information system security, categorizing the threats based on their sources, perpetrators, intent and consequences, as shown in Figure 1:

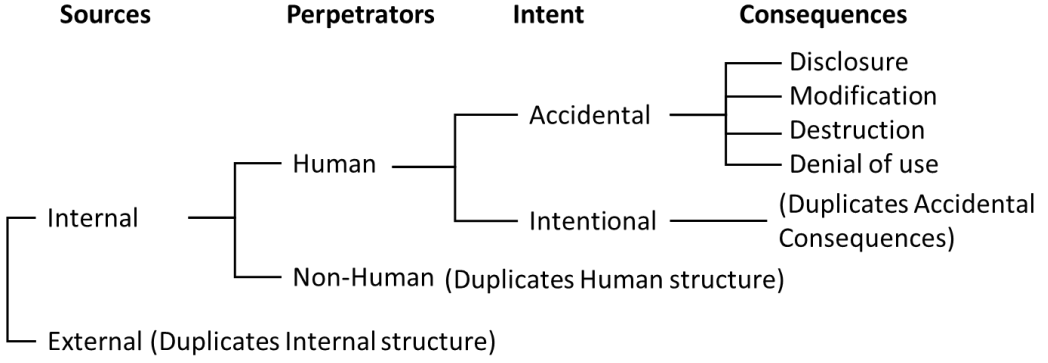

Figure 1: The Four Dimension of Information Systems Security (Lock, Carr & Warkentin, 1992)

Willison, R. & Warkentin, M. (2013) Beyond Deterrence: An expanded View of Employee Computer Abuse. MIS Quarterly 37(1), March, 1-20.

In this Research Commentary, the authors expand upon the Loch et al. study focusing on employee or insider behavior. While focusing on research questions of "*rationalizations associated with specific forms of employee computer abuse; techniques of neutralization that predict employee's intention to commit computer abuse, and relationships between techniques of neutralization and computer*," the authors begin by providing a refined version of the Loch, et al IS Security Threat Vector Taxonomy, as shown in Figure 2.

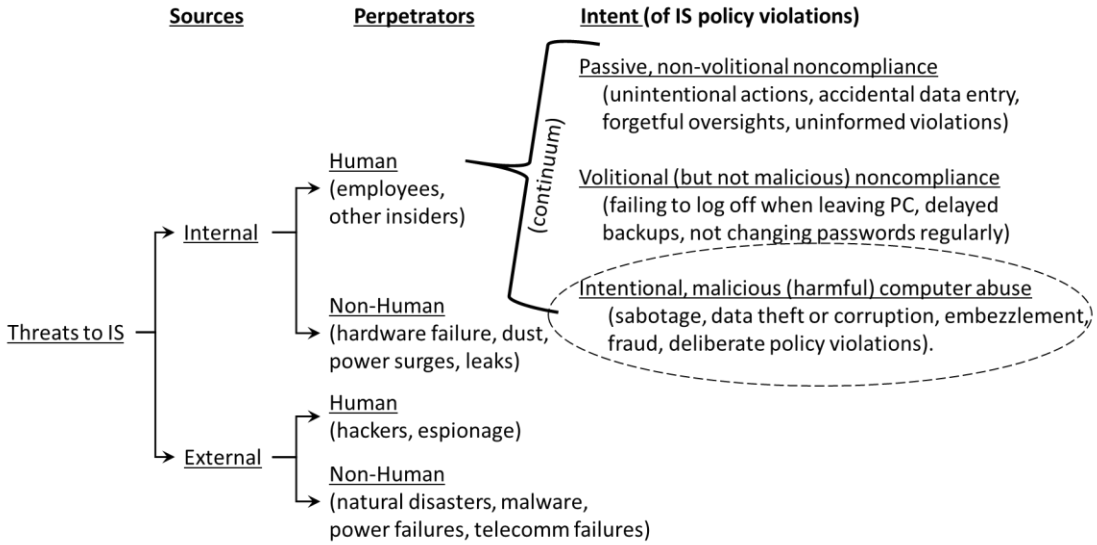

Figure 2: IS Security Threat Vector Taxonomy (Willison & Warkentin, 2013)

Jouini, M., Ben Arfa Rabai, L., & Ben Aissa, A. (2014) Classification of security threats in information systems, 5th International Conference on Ambient Systems, Networks and Technologies. Procedia Computer Science 32 pp. 489-496.

(Note these authors published a continuation paper the following year at the same conference).

This paper proposes a "multi-dimensional threats classification model" extending previous works, including Loch, Carr and Warkentin (1992), as shown in Figure 3. The article modifies the classifications of Human vs Non-Human of Loch et al, and adds a new dimension of Malicious vs. Non-Malicious, as an extension of the foundation paper's Intent category.

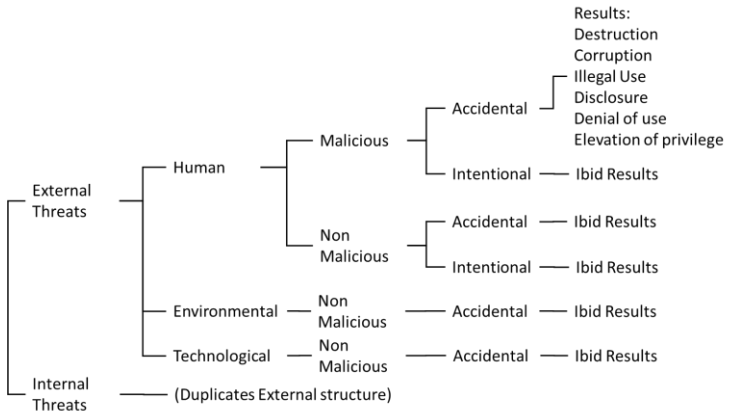

Figure 3: The multi-dimensions threats classification model (Jouini et al, 2014)

INDUSTRY PERSPECTIVES ON THREATS

Studies of threats to information security are popular in industry, especially among consulting organizations. These studies are also the foundation for academic research (s.f. Liang & Xue, 2009; Willison & Warkentin, 2013, Kim & Kim, 2014; Wang, Gupta & Rao, 2015; et al.) One sequence is particularly significant because of its widespread recognition and the number of years it persisted.

CSI Computer Crime and Security Survey (CSI, 1999-2011)

Considered the definitive authority on security threat surveys, the CSI Computer Crime and Security Survey from the Computer Security Institute ran from 1996 until mid-2011, when the Institute was subsumed by UBM TechWeb and the survey discontinued. Until that time, CSI conducted annual polls, jointly with the FBI's Computer Intrusion Squad until 2005. Although some claim the methodology used by CSI has issues of sample control, as, like most industry security surveys, the study is based on a predefined membership, in this case the CIS membership rolls and attendees at paid CSI conferences and training events. Other reported issues included reported sample size, as CSI purportedly reports a sample of over 5000, yet the actual response rates were regularly in the 300-750 range. Not an issue of survey size, but of *reported* survey size (Winkler, 2006). These issues were formally addressed in the latter years of the survey. Regardless of these concerns, many articles, textbooks and research papers have cited this work over the years. Table 1 provides an overview of the threats reported by respondents of the CSI surveys from 1999 until its cessation in 2010/11.

Type of Attack or Misuse	2010/11	2009	2008	2007	2006	2005	2004	2003	2002	2001	2000	1999
Malware infection (revised after 2008)	67%	64%	50%	52%	65%	74%	78%	82%	85%	94%	85%	90%
Being fraudulently represented as sender of phishing message	39%	34%	31%	26%	(new category in 2007)							
Laptop/mobile hardware theft/loss	34%	42$ %	42%	50%	47%	48%	49%	59%	55%	64%	60%	69%
Bots/zombies in organization	29%	23%	20%	21%	(new category in 2007)							
Insider abuse of Internet access or e-mail	25%	30%	44%	59%	42%	48%	59%	80%	78%	91%	79%	97%
Denial of service	17%	29%	21%	25%	25%	32%	39%	42%	40%	36%	27%	31%
Unauthorized access or privilege escalation by insider	13%	15%	(revised category in 2009)									
Password sniffing	11%	17%	9%	10%	(new category in 2007)							
System penetration by outsider	11%	14%	(revised category in 2009)									
Exploit of client Web browser	10%	11%	(new category in 2009)									
Attack/Misuse categories with less than 10% responses as of 2010/2011 survey (listed in decreasing order):												
Financial fraud												
Web site defacement												
Exploit of wireless network												
Other exploit of public-facing Web site												
Theft of or unauthorized access to PII or PHI due to all other causes												
Instant Messaging misuse												
Theft of or unauthorized access to IP due to all other causes												
Exploit of user's social network profile												
Theft of or unauthorized access to IP due to mobile device theft/loss												
Theft of or unauthorized access to PII or PHI due to mobile device theft/loss												
Exploit of DNS server												
Extortion or blackmail associated with threat of attack or release of stolen data												

Table 1: CSI Survey Results: Threats 1999-2011 (CSI, 1999-2011)

In the last two years, many organizations published studies, surveys, white papers or reports related to threats information protection or information security. These included the following (listed in alphabetical order):

Australian Cyber Security Center's 2015 Cyber Security Survey (ACSC, 2015)

This study drew responses from 149 organizations across 12 business sectors in Australia. As shown in Table 2, when asked to identify what threats caused the most frequent incidents in their organizations, 72 percent of the respondents chose ransomware, fully a quadrupling of the number from 2013. Respondents were found to have reported ransomware as having impacted every one of the 12 business sectors represented by the respondents.

Most prevalent types of Incidents	2015	2013	2012
Ransomware	72%	17%	
Malware	66%		
Targeted malicious emails	59%	63%	
Virus or worm infection	30%	52%	28%
Theft of mobile devices and laptops	30%	35%	32%
Trojan	27%	46%	21%
Remote access Trojans (RATs)	20%		
Unauthorized access	25%	26%	18%
Theft or breach of confidential information	23%		17%
Unauthorized access to information from an outsider	17%		
Denial of service attack	16%	17%	16%
Unauthorized access to information from an insider	14%	17%	
Number of Survey Respondents (Organizations): 2015 - 149, 2013 - 135. 2012 - 255			

Table 2: 2015 Australian Cyber Security Center Survey: Major Australian Businesses (ACSC, 2015)

Computer Economics Insider Misuse of Computing Resources (Computer Economics, 2009)

While this report is from data collected several years ago, it still offers a unique approach to classifying the types of insider misuse. The report is based on data collected by survey from 100 IT security professionals and executives from around the world. It examines the threat of insider misuse of computing resources. As shown in Table 3, for each of 14 types of insider misuse, the report assesses the perception of the seriousness of the threat and how organizations usually deal with that type of misuse in policy.

Insider Misuse	Percentage
Portable Storage Misuse	57%
Software Downloading	56%
P2P File-Sharing	54%
Remote-Access Programs	53%
Rogue Wi-Fi Access Points	48%
Rogue Modems	47%
Media Downloading	40%
Personal Devices	40%
Unauthorized Blogging	25%
Personal IM Accounts	24%
Message Board Posting	19%
Personal Email Accounts	16%
Non-Work Web Browsing	14%
Business Email Misuse	6%

Table 3: Percentage of Organizations Viewing Type of Insider Misuse as Major Threat (Computer Economics, 2009)

Some key findings were that unauthorized use of portable storage devices for copying files is a major source of losses and is the most serious threat encountered yet one-third of organizations do not attempt to deter these activities. A close second as a threat is the downloading of unauthorized software with almost 90% of organizations forbidding that activity by policy. Also of concern are the unauthorized use of P2P file-sharing programs and the use of unauthorized remote access programs and services.

CyberEdge Group Cyber Threat Defense Report (CyberEdge, 2016)

While this report focuses on defensive actions taken by organizations from around the world it also explores the threat landscape by asking 1,000 IT security managers and professionals, each from an organization with more than 500 employees from 10 countries across North America, Europe, Asia Pacific, and Latin America. The respondents came from 19 industry sectors.

When asked about their organization's concerns for anticipated cyber threats, they reported that threats in social media applications, cloud-based technologies and mobile-devices deployments are widespread and growing. Details of their responses are shown in Table 4. Items of note also included a report that only 20 percent of organizations achieve meaningful level of backups of user's mobile device contents, less than one-third or security professionals believe that their organizations have sufficient controls on privileged user accounts, and ninety percent of respondent believe that malware control approaches as deployed are inadequate to the level of threat.

On a scale of 1 to 5, with 5 being highest, rate your overall concern for each of the following types of cyber threats targeting your organization.	**2016**	**2015**	**2014**
Malware (viruses, worms, Trojans, ransomware)	3.93	3.39	3.26
Phishing / spear-phishing attacks	3.81	3.44	3.26
SSL-encrypted threats	3.72	3.21	n/a
Denial of service (DoS/DDoS) attacks	3.69	3.1	2.91
Advanced persistent threats (APTs) / targeted attacks	3.69	3.23	2.94
Web application attacks (buffer overflows, SQL injections, cross-site scripting)	3.67	3.26	3.1
Zero-day attacks (against publicly unknown vulnerabilities)	3.64	3.38	3.1
Watering hole attacks	3.54	3.11	n/a
Drive-by downloads	3.5	2.99	n/a
Number of Survey Respondents: 2016 - 986, 2015 - 793. 2014 - 649			

Table 4: Top Cyber Threats 2014-2016 (CyberEdge, 2016)

- **Dell Security Annual Threat Report (Dell, 2016)**

Dell's report observes that the major breaches in the recent past have been at organizations with operating security infrastructure that had small vulnerabilities exploited in big ways. The report does not offer statistical results in ranking threats. The information used in the report was gathered by Dell's SonicWALL Global Response Intelligence Defense (GRID) Network summarizing over 1 million security sensors in nearly 200 countries and territories and augmented with additional sources.

The key findings of the report are summarized info five points: 1) Attack scripts and exploit kits are evolving to be faster and more novel to stay ahead of currently deployed control systems with ever more variety in malware attacks having the number of unique malware variants from 37 million variants used in 4.2 billion in 2014 attacks to 64 million variants used in 8.19 billion attacks in 2015, 2) The trend to more widespread usage of Secure Sockets Layer/Transport Layer Security (SSL/TLS), nominally an improvement for security, has formed an infrastructure that enables stealthy "hackware" command and control to facilitate broader attacks from that threat, 3) Android smartphone architectures are seeing increased levels of attack putting most of the smartphone user market at greater risk, and 4) Malware attacks continue to grow in volume and sophistication.

Ernst & Young Global Information Security Survey (Ernst & Young, 2015)

In Ernst & Young's most recent annual survey, 1,755 respondents in 67 countries were asked to rank their perception of various threats and vulnerabilities. As shown in Table 5, looking only at the threats ranked at the highest level by respondents, phishing and malware were viewed as the largest threats where in prior years this threats were reported as 5th and 7th respectively.

Rounding out the top tier of threats in this study are zero day attacks, cyberattacks focused on theft, cyberattacks focused on disruption and what some would consider cyber-enable fraud. Of note in this report is what survey respondents viewed as the highest priority threats for the coming year where they identified data loss prevention, business continuity, and access management as the top three.

Threat	2015 Percent Ranking Highest	2014 Percent Ranking Highest
Phishing	19%	17%
Malware	16%	15%
Zero-Day attacks	16%	16%
Cyber attacks to steal financial information	15%	28%
Cyber attacks to disrupt or deface	15%	25%
Cyber attacks to steal intellectual property or data	13%	20%
Fraud	12%	19%
Natural disasters	9%	15%
Espionage	9%	16%
Spam	9	13

Internal attacks	9	11
Number of Survey Respondents: 2015 - 1755. 2014 -1825		

Table 5: Percentage of Respondents Ranking Threat as Highest (Ernst & Young, 2015)

IBM Cyber Security Intelligence Index (IBM, 2016)

This report discusses threats only in the context of broader themes. Yet, IBM Security Services prepared these observations from data aggregated from continuously monitoring billions of events over the course of 2015 relying on 8,000 client devices in over 100 countries. One observation asks "*Who are the threat agents?*" Table 5 shows that 60% of attacks are from those with a relationship to the organization with that percentage increasing from 55% in 2014. These threat agents pose a significant threat in both financial and reputational terms.

Threat Agencies?	**2015**	**2014**
Outsiders	40%	45%
Insiders	60%	55%
Malicious Insiders	44.5%	31.5%
Inadvertent actors	15.5%	23.5%

Table 6: Threat Agencies (IBM, 2016)

Another aspect of the threat landscape that IBM reported on was that of the type of incidents that were reported. As Table 6 shows, when selected from the largest five industry sectors in the data, unauthorized access incidents continue to top the list and grew in frequency.

Incident Types	**2015**	**2014**
Unauthorized access	45%	37%
Malicious code	29%	20%
Sustained probe/scan	16%	20%
Suspicious activity	6%	11%
Access of credentials abuse	3%	8%

Table 7: Percentage of Respondents Reporting Incident Types (IBM, 2016)

InformationWeek Strategic Security Survey (2015)

InformationWeek and DarkReading's Report for 2015 identified Cybercriminals as their top security threat, similar to the result for 2014. A few points made in the report are IT Systems complexity continues to grow in the opinion of 44% of the 435 respondents from North American businesses that took the survey. It is believed that increasing complexity one factor that has led to an increasing number of successful attacks. The survey also found that 65% of those responding felt they were more vulnerable at the moment than in the past. Of significance was that fully 15% of those responding had a breach or compromise with estimates of the cost of ranging from $500,000 and a $1 million. 6% of those respondents reporting a breach indicated the losses were $5 million or more. The sources of breaches were identified by participants in the study as being mostly 'cybercriminals' as shown in Table 8.

Which of the following possible sources of breaches or espionage pose the greatest threat to your organization this year?	**2015**	**2014**
Cybercriminals	60%	56%
Authorized users or employees	45%	49%
Application vulnerabilities	42%	40%
Public interest groups or hactivists	22%	21%
External users	17%	19%
Contracted service providers, consultants or auditors	16%	17%
Foreign governments	15%	13%
Competitors	12%	13%
Customers	11%	13%
Our own government	3%	6%
Other	1%	2%
Unknown	6%	5%
Note: Maximum of 3 responses allowed.		
Number of Survey Respondents: 2015 - 435, 2014 - 536		
InformationWeek survey of organizations with 100 or more employees		

Table 8: Top Security Threats (InformationWeek, 2015)

ISACA/RSA State of Cybersecurity Implications for 2016 (ISACA, 2016)

In anticipation of the annual RSA conference ISACA and the RSA Conference conducted a global survey of 461 cybersecurity managers and practitioners in November and December of 2015. The key results of this survey revealed that respondent believed the number of data breaches revealing organizational and individual data are unchecked and continue to grow while the attack methodologies evolve toward every more complex, subtle and sophisticated methods. Cybersecurity as practiced is a chaotic process and attacks against information assets are expected to continue to grow in number and in realized losses. Nearly 75 percent of participant in the study expect to realize some type of loss from cyberattack in 2016. The report notes that cybercriminals are the most numerous of the types of attackers and they use social engineering as their primary means of initiating attacks.

When asked to identify the type and frequency of malicious activities in the past year, respondents identified malware as the most frequent daily occurrence as shown in Table 9.

Type and Frequency of Malicious Activity Occurrences in 2015	Daily	Weekly	Monthly	At least quarterly	N/A
Online identity theft	4%	5%	6%	21%	65%
Hacking	11%	7%	9%	25%	47%
Malicious code	16%	12%	13%	26%	32%
Loss of intellectual property	1%	2%	4%	20%	72%
Intentional damage to computer systems	1%	1%	5%	18%	74%

Table 9: RSA Conference State of Cybersecurity 2016 Type and Frequency of Malicious Activity Occurrences (ISACA, 2016)

Kaspersky Consumer Security Risks Survey (Kaspersky, 2015a)

Kaspersky Lab working with the B2B International research firm explored how global Internet users anticipate and are affected by current online threats. The study explores how devices are used to leverage the Internet and looks at what consumers think of current Cyber threats. The study surveyed 12,355 people (11,344 excluding China) aged 16 and over, balancing responses of men and women. The data was weighted to be globally representative and consistent.

The study found that consumers perceive risk as categories of malware, identity theft/account hacking and financial incidents. Respondents suffered at least one malware incident in the last 12 months at least 45% of the time. While many could recall how they were compromised, 13% of those who became infected didn't know how it occurred. Over a third (36%) reported exposure to an identity threat with primary approach continues to be a pretense with attackers representing themselves falsely in order to convince people to reveal personal information. A quarter (25%) of those surveyed encountered account hacking of some nature in the previous year. Over one tenth (11%) of respondents lost control of email or social media accounts and 7% lost control of and online banking or shopping account.

Among those losing control of accounts, nearly a third of those hacked had unauthorized messages sent from the compromised account. Over a quarter found their accounts used as malware vectors, sending attachments (29%). A similar number discovered that information had been deleted or stolen for some criminal purpose (26%).

Kaspersky IT Risks Survey (Kaspersky, 2015b)

Another report form Kapersky and B2B International, the Kaspersky Lab's Global IT Security Risks Survey, is in its 5th year gathering responses from global IT professionals. This report serves as a look at the attitudes of informed IT industry professionals regarding security revealing what they think about the type and level of IT security threats they face. The study gathered responses from 5564 respondents from 38 countries collected in April 2014 and May 2015.

Some notable finding from the study are that over 90% of businesses have experienced some form of external threat and 22% of businesses report losing data as a result of an external threat. On the other hand, there have been fewer instances of theft and 'obvious' malware than in the prior year and organizations losing data as a result of malware were reduced to 25% from 33% in the prior year. The report also found that 17% of organizations currently outsource IT security decisions, relying on external expertise.

Ponemon Cost of Cyber Crime Study Global (Ponemon, 2015)

Hewlett Packard sponsored the Ponemon 2015 Cost of Cyber Crime Study: Global where 252 organizations with a minimum of approximately 1,000 enterprise seats generated this benchmark analysis. This report found that cyber crimes continue to be on the rise for those organizations measured with the mean annualized cost of cyber crime at $7.7 million per year where the prior year mean cost was $7.6 million, or a 1.9 percent net change. The study found that cyber crime cost varies by the size of the organization with a positive relationship between organizational and annualized cost. It is noted that small organizations incur a significantly higher per capita cost than larger organizations ($1,388 versus $431). Costs vary by industry segment, where healthcare, automotive and agriculture organizations incur lower costs that those in financial services and utilities & energy which have substantially higher cyber crime costs.

The study found that the costliest cyber crimes are from malicious insiders with other higher cost categories being denial of services and web-based attacks. Rapid resolution was found to be one way to avoid higher costs of cyber since the report found a positive relationship between the time to contain an attack and organizational cost. On investigation it was found that business disruption represents the highest element of external cost at 39%, followed by the costs associated with information loss.

Ponemon Global Megatrends in Cybersecurity (Ponemon, 2015b)

2015 Global Megatrends in Cybersecurity was prepared by Ponemon and sponsored by Raytheon. The study was designed to document larger trends and changes over the subsequent three years as it surveyed 1,006 senior-level information technology and information technology security leaders familiar with their organizations' cybersecurity strategies from multiple countries.

The study reported on seven mega trends as follows:

1. Cybersecurity will become a competitive advantage and a C-level priority.
2. Insider negligence risks are decreasing as organizations gain better control over employees' insecure devices and apps.
3. Cybercrime will keep information security leaders up night since significant increases in the risk of nation state attackers and advanced persistent threats will continue.
4. The Internet of Things is here but organizations are slow to address its security risks.
5. The cyber talent gap will persist.
6. New technologies like big data analytics, advances in forensics and intelligence based cyber solutions will drive innovation in security control systems.

7. Cybersecurity postures are expected to improve even as media headlines show increasing alarm.

Table 10 shows what the study reports as the most prevalent types of cyber threats anticipated for the next 3 years with the five most prevalent expected to be zero day attacks, data leakage in the cloud, mobile malware/targeted attacks, SQL injection and phishing attacks.

Cyber Threat or Attack	Percentage of Respondents
Zero day attacks	49%
Cloud data leakage	41%
Mobile malware/targeted attacks	38%
SQL injection	37%
Phishing attacks	36%
Critical infrastructure attacks	35%
Watering hole attacks	29%
Comprised supply chain	25%
Insider threats	23%
DDos	23%
Rootkits	22%
BYOD data theft	13%
Cross-site scripting	12%
Compromised trusted partners	10%
Compromised MSSPs/SaaS providers	10%
MacOS malware/targeted attacks	10%
Botnet attacks	9%
Linux malware/targeted attacks	8%
Clickjacking	8%
Attacks against control systems	7%

Table 100: What respondents believe will be the most prevalent cyber threats or attacks over the next three years (Raytheon, 2015)

PricewaterhouseCoopers/CERT 2015 US State of Cybercrime Survey (PwC, 2015)

PricewaterhouseCoopers co-sponsored this survey of cybercrime in 2014 with the U.S. Secret Service, CSO magazine and Carnegie Mellon University's CERT® division of the Software Engineering Institute. The survey includes reactions from some 500 respondents including a variety of security professionals from both the private and public sectors. The "big take-away" from this survey is that 76% of respondents in the 2015 survey indicated they were more concerned this year than in the previous year about cybersecurity threats. The previous year's response to the same question was only 59%. Table 11 provides the results of the question "what is the greatest cyber threat to your organization?"

What is the greatest cyber threat to your organization?	2014	2013
Hackers	25%	24%
Current employees	12%	13%
Organized crime	10%	8%
Foreign nation-states	8%	7%
Activists/hacktivists	6%	5%
Do not know	23%	23%

Table 111: Greatest cyber threats to organizations (PwC, 2015)

Verizon Data Breach Investigations Report (Verizon, 2016)

Sponsored predominantly by Verizon, the 2016 Data Breach Incident Report assessed over 100,000 incidents over 82 countries of which over 3140 were confirmed data breaches. Table 12 shows the number of breaches per threat action bi-annually since 2011.

Number of Breaches per threat action category	2015	2013	2011
Hacking	~1600	~950	~550
Malware	~1325	~825	~450
Social	~800	~450	~200
Error	~250	~165	~80
Misuse	~200	~175	~150
Physical	~150	~175	~160
Environmental	~30	~30	~30
Note numbers estimated from non-specific charts provided in reports			

Table 12: Number of breaches per threat action category over time (Verizon, 2016)

Table 13 shows threat action varieties in breaches annually over the past three years.

Threat action varieties in breaches	2015	2014	2013
Malware - C2	~1020	~130	~160
Hacking - Use of stole creds	~1000	~275	~520
Malware - Export data	~960	~175	~360
Hacking - Use of backdoor or C2	~960	~240	~200
Social - Phishing	~920	~475	~280
Malware - Spyware/Keylogger	~830	~100	~180
Malware - RAM	~440	~550	~320
Hacking - Brute force	~290	~420	~130
Malware - Backdoor	~180	~140	~200

Note numbers estimated from non-specific charts provided in reports

Table 13: Threat action varieties in breaches over time (Verizon, 2016)

ACADEMIC PERSPECTIVES ON THREATS

Industry sources tend to be more proactive in the identification and classification of threats to information protection, thus there are correspondingly more articles focused on the specific identification of threats. In the world of academic analysis, there are many articles that try to describe or understand the human factors such as the "insider threat" (s.f. Baracaldo and Joshi, 2013; Harrington, 1996; Huth et al., 2013; Loch et al., 1992; Straub, 1990; Wang et al., 2008; Warkentin and Willison, 2009). There are a few prominent articles that specifically look to identify and/or categorize the threats to information protection and are thus included here. Additional criteria for inclusion in this list included the type and quality of the journal, with a focus on scholarly articles in mainstream computing peer-reviewed academic venues. The articles are listed in chronologic order.

Hoffer, J. A. and Straub, D. W. (1989) The 9-5 Underground: Are You Policing Computer Crimes? Sloan Management Review. 30, 4 (Summer), 35-43.

One of the earliest studies of threats to then information (data) security, this study examines attitudes toward computer systems abuse in the organization, specifically looking at the following questions:

"*To whom is data system abuse being reported?; How are systems being abused?; Who are the abusers, and what motivates them?; Are privileged personnel more prone to abusing systems than other users?; Is organizational size a factor in how much abuse occurs?; Are certain industries more susceptible to abuse than others? What measures can be taken to deter abuses?; Can administrative as well as operational measures be effective?*" (Hoffer & Straub, 1989).

The study invited almost 5,500 randomly selected managers from within the Data Processing Management Association (DPMA) membership to participate in the survey and received in over 1200 responses. The study found the predominance of threats at the time were from internal abuse or misuse of computer systems from within five categories of unauthorized use of computer service, disruption of computer service, and abuse affecting data, programs and hardware. The study also noted the evolution of a new brand of threat at the time – the computer virus.

Loch, K. D., Carr, H. H., and Warkentin, M. E. (1992) Threats to information systems: Today's reality, yesterday's understanding. MISQ. 16, 2, 173–186.

Considered to be one of the seminal studies on information security threats, this article sought to address two questions: "*(1) What are the threats to information systems and resident data?* [and] *(2) Which of these are the most serious threats?*" (Lock, Carr and Warkentin, 1992). Based on a literature review of threats and subsequent review by security executive and consultants, the study looked at the threats to information systems security including three main domains: mainframe, microcomputer and network. The study surveyed security managers from the Atlanta, Georgia area for the pilot and then the entire country for the main study, all drawn from the Directory of Top Computer Executives. Their findings are shown in Table 14:

		Microcomputer Weighted Votes			**Mainframe Computer Weighted Votes**			**Networks Weighted Votes**		
Threats (by Environments)	**Ext/Int**	**Nr.**	**% Tot**	**Rank**	**Nr.**	**% Tot**	**Rank**	**Nr.**	**% Tot**	**Rank**
Natural disasters	E	74	11.7%	4	135	21.3%	2	115	31.3%	1
Accidental entry bad data by employees	I	112	17.7%	2	158	24.9%	1	-	-	-
Accidental destruction data by employees	I	137	21.6%	1	115	18.1%	3	-	-	-
Weak/ineffective controls	I	52	8.2%	5	17	2.7%	9	80	21.7%	3
Entry of computer viruses	E	50	7.9%	6	13	2.0%	11	65	17.7%	4

Access to system by hackers	E	16	2.5%	10	20	3.1%	8	87	23.6%	2
Inadequate control over media	I	80	12.6%	3	16	2.5%	10	-	-	-
Unauthorized access by employees	I	38	6.0%	7	55	8.7%	4	-	-	-
Poor control of I/O	I	31	4.9%	8	36	5.7%	5	-	-	-
Intentional destruction data by employees	I	23	3.6%	9	35	5.5%	6	-	-	-
Intentional entry bad data by employees	I	10	I.6%	11	26	4.1%	7	-	-	-
Access to system by competitors	E	9	1.4%	12	6	0.9%	12	16	4.3%	5
Other threats		2	0.3%	13	3	0.5%	13	5	1.4%	6
Totals		634			635			368		

Table 14: Threat Ranking for Each Environment (Weighted Vote Method) (Loch, Carr & Warkentin, 1992)

Straub, Jr., D. and Welke, R. (1998) Coping with systems risk: Security planning models for management decision making. MIS Quarterly. 22(4), 441–469.

This study represents a risk-based approach to understanding threats to security, as a fundamental component of understanding the security problem. The authors conducted qualitative interviews of two Fortune 500 organizations over a 15 month period, attempting to understand two propositions: "*Proposition 1: Managers are aware of only a fraction of the full spectrum of actions that can be taken to reduce systems risk. Proposition 2: Managers exposed to theory-grounded security planning techniques will be inclined to employ these in their planning processes*" (Straub & Welke, 1998). The result of the study was "a theory-based security program that includes (1) use of a security risk planning model. (2) education/training in security awareness, and (3) Countermeasure Matrix analysis" (Straub & Welke, 1998). The authors specifically asserted that techniques such as threat tree analysis are a recommended practice as a component of a risk assessment program.

Whitman, M. (2003). Enemy at the Gates: Threats to Information Security. *Communications of the ACM, 48*(8), 91-95.

In 2002, the author sought to update and extend the work of Loch, Carr and Warkentin (1992). The study identified a dozen categories of threats to information security from over 215 candidate threat categories from previous literature, industry reports and other venues. The primary research questions posed were: "*(1) What are the threats to information security?; (2) Which of these threats are the most serious; (3) How frequently (per month) are these threats observed?* [and] *(4) Which threats represent the highest attack-driven expenditures?*" (Whitman, 2003). The study conducted a pilot study soliciting responses from 150 Atlanta area chief computer executives from the Directory of Top Computing Executives. The full study polled over 1000 senior computer executives, with 192 usable responses. The findings from the first two questions are presented in Table 15.

Threat	Mean	Std. Dev	Weight	Weighted Rank
Deliberate Software Attacks	3.99	1.03	546	2178.3
Technical Software Failures or Errors	3.16	1.13	358	1129.9
Act of Human Error or Failure	3.15	1.11	350	1101.0
Deliberate Acts of Espionage or Trespass	3.22	1.37	324	1043.6
Deliberate Acts of Sabotage or Vandalism	3.15	1.37	306	962.6
Technical Hardware Failures or Errors	3.00	1.18	314	942.0
Deliberate Acts of Theft	3.07	1.30	226	694.5
Forces of Nature	2.80	1.09	218	610.9
Compromises to Intellectual Property	2.72	1.21	182	494.8
Quality of Service Deviations from Service Providers	2.65	1.06	164	433.9
Technological Obsolescence	2.71	1.11	158	427.9
Deliberate Acts of Information Extortion	2.45	1.42	92	225.2

Table 15: Weighted Ranks of Threats to Information Security (Whitman, 2003)

Keller, S., Powell, A., Horstmann, B., Predmore, C., and Crawford, M. (2005). Information Security Threats and Practices in Small Businesses. *Information Systems Management,* Spring, 7-19.

This study focuses on threats specific to small businesses of fewer than 500 employees. The research questions include: "*What are the current threats and trends associated with computer asset attacks, and what are the implications of such threats?; What steps are small businesses taking to secure their computer systems, and how do they compare to published "best practices?"; and "Do these small businesses have an Emergency Action Plan with respect to IT security?"* (Keller et al., 2005). The study interviewed representatives from eighteen small businesses in a nearby metropolitan area. The study's findings to its first research question are presented in Table 16.

Threat	Percent
Internal	55.6%
Trojans	27.8%
Hackers	22.2%
Viruses	22.2%
Password Control	5.6%
Microsoft Vulnerabilities	5.6%
Spyware/Malware	5.6%
No Threats	16.7%
Number of Interview Respondents: 18	

Table 16: Perceived Data Security Threats (Keller, 2005)

Many of the study's respondents indicated that because they were a small business, they were not at as much of a target as larger organizations are.

Whitman, M., & Mattord, H. (2012). Threats to Information Security Revisited. *Journal of Information Systems Security, 8*(1), 21-41.

As a decade-later update to the Whitman (2003) study, this article surveys industry to determine if the threats observed in 2002 are still dominant in business. The study replicated the methodology of the previous study, sending email invitations to over 1000 top computing executives, randomly selected and invited to participate in an online survey from the Directory of Top Computing Executives. The study sought to revisit the findings of the 2002 study asking "*a) Have the threats to information security changed in priority?; b) What risk management efforts organizations now employ?* [and] *c) What standards influence information security efforts?*" (Whitman & Mattord, 2012). A total of 141 responded. The study's findings are presented in Table 17:

2010 Overall Rank	Categories of Threats	2010 Rate	2002 Rate	2010 Rank	2002 Rank	2010 Combined	2002 Combined	2002 Overall Rank
1	Espionage or Trespass	3.54	3.22	462	324	16.35	10.43	4
2	Software Attacks	4.00	3.99	306	546	12.24	21.79	1
3	Human Error or Failure	4.30	3.15	222	350	9.55	11.03	3
4	Theft	3.61	3.07	162	226	5.85	6.94	7
5	Compromises to Intellectual Property	3.59	2.72	162	182	5.82	4.95	9
6	Sabotage or Vandalism	3.11	3.15	111	306	3.45	9.64	5
7	Technical Software Failures or Errors	3.17	3.16	105	358	3.33	11.31	2
8	Technical Hardware Failures or Errors	2.88	3.00	87	314	2.51	9.42	6
9	Forces of Nature	2.76	2.80	81	218	2.24	6.10	8
10	Quality of Service Deviations from Service Providers	2.88	2.65	72	164	2.07	4.35	10
11	Technological Obsolescence	2.66	2.71	57	158	1.52	4.28	11
12	Information Extortion	2.68	2.45	18	92	0.48	2.25	12

Table 17: 2002 and 2010 Studies Compared (Whitman & Mattord, 2012)

Sumner, M. (2009). Information Security Threats, A Comparative Analysis of Impact, Probability, and Preparedness. Information Systems Management, 26: 2-12.

This study adopts the threats presented in Whitman, 2003, and seeks "*(1) to determine the risk assessment of information security threats, based upon the perceived impact and the perceived probability of occurrence of these threats; (2) to determine the extent of risk mitigation, based upon the perceived level of preparedness for each of these information security threats;* [and] *(3) to determine the extent to which the of occurrence and the impact of information security threats relate to the level of preparedness*" (Summer, 2009). In a survey of 102 IT professionals, the study plots mean responses on a 2x2 probability by impact rating scale of Low vs. High, with the results shown in Table 18. The study's findings support current risk management methodologies in threat assessment using the impact times probability ratings.

Legend	Impact	Impact Level	Prob	Prob Level	Quad	Prep	Prep Level
Human Error	4.57	High	4.65	High	4	4.66	2
Intellectual Property Infringement	4.24	High	3.43	Low	3	4.27	2
Acts of Trespass	5.37	High	3.15	Low	3	4.71	2
Acts of Information Sabotage	5.23	High	2.84	Low	3	4.65	2
Acts of Sabotage or Vandalism	5.79	High	2.99	Low	3	4.77	2
Acts of Theft	5.13	High	3.37	Low	3	4.73	2
Software Attacks	5.15	High	4.22	High	4	5.28	3
Forces of Nature	5.23	High	3.63	High	4	4.7	2
Quality of Service Deviation	4.87	High	4.05	High	4	4.65	2
Tech Hardware Failure	4.63	High	4.56	High	4	5.21	3
Tech Software Failure	4.63	High	4.4	High	4	4.98	3
Tech Obsolescence	3.8	High	4.38	High	4	4.63	2

Table 18: Mean Scores of Impact, Probability, and Preparedness (By Quadrant) (Sumner, 2009)

While these articles represent a small portion of those published on threats, they do represent the bulk of the articles focused on identifying threats. There are many other relevant articles on modelling threats, assessing threats and understanding threats; however, these were determined to be beyond the scope of this review.

2015 SEC/CISE STATE OF THE INDUSTRY REPORT RESEARCH

Mattord, H. and Whitman, M. (2015) 2015 SEC/CISE Threats to Information Protection Report Including a Current Snapshot of the State of the Industry. Security Executive Council.

In 2015, the Kennesaw State University Center for Information Security Education, in cooperation with the Security Executive Council (www.security executivecouncil.com) began a project to define and document the State of the Industry with regard to Information Protection. The resulting report reviewed industry sources for changes in the information protection threat landscape. As part of this project, the Center conducted an independent research study to identify current trends in information protection. The study asked practitioners about their perceptions of current threats to information protection. The study was funded in part by the by the Coles College of Business Research and Development program, and conducted within the guidelines of the Kennesaw State University Institution Review Board. Portions of that report are included here with permission.

In order to continue and extend the work of previous studies (Whitman, 2003; Whitman & Mattord, 2012), a new survey was developed and administered in 2015. Using the Whitman (2003) survey as a starting point, questions on information security positions were added, along with organizational demographic questions on the maturity of key security program components. The survey was examined by a panel of security researchers, and recommended revisions implemented. Titled the "2015 Bi-Annual SEC/CISE Survey of Threats to Information Protection" (Whitman & Mattord, 2015) the study was conducted between January and April 2015. The study polled over 12,000 industry professionals, and involved sending email invitations to potential respondents, based on lists acquired from the readerships of popular information security journals, and the SEC's internal membership database. The target respondents were identified as individuals with job descriptions or positions associated with security management in the organization, including Chief Information Security Officers (CISO), Chief Security Officer, Director of IT Security or Information Security, Manager of IT security or Information Security or other related title. Reminders to participate in the survey were emailed at approximately one month intervals for three months.

Survey Demographics

267 responses were received during the survey period. Respondents were predominantly from the USA (64.8%) with 4.5% from North America (except USA), 1.1% from Central and South America, .7% from Western Europe (except UK) and .4% from Africa/Middle East and Eastern Europe. 28.1% of respondents elected not to share their locale.

Respondents represented organization with a variety of organizational sizes but the bulk of the respondents came from organizations with more than 5000 employees (48%). The remainder was from organizations with 1-49 employees (9%); 50-999 (19%); 1000-2499 (11%) and 2500-4999 (48%). Respondents represented multiple sized organizations with gross revenues across the board, the largest group being over $50m (62.3%) of those providing this information. The remaining organizations represented were relatively evenly distributed from the very small (under $10,000) through the $30m-$50m category.

Respondents represented a wide range of business activities, with Education (18%), Other or Multiple Groups (11.6%), Banking/Finance/Accounting (7.1%), Medical/Dental/Healthcare (6.0%) and State/Local Government (5.2%) representing the largest individual business groups out of the 20 options provided.

Survey Findings

Cybersecurity Staffing and Personnel

With such a large average organizational size one would expect a commensurately large information security group. However, the response to the question "How many full-time information security employees are there in your entire organization at this time?" found surprisingly few full time employees per organization, and a disturbing number with none. Table 19 shows the number of full time information security professionals by organizational size (based on number of employees):

151 responses		**# of full-time information security professionals**							
		0	1-5	6-10	11-25	26-50	51-100	101 or more	% of total resp.
# of employees	1 - 49	33.3%	58.3%	8.3%	0.0%	0.0%	0.0%	0.0%	8%
	50 - 999	7.1%	67.9%	17.9%	3.6%	0.0%	0.0%	3.6%	19%
	1,000 - 2,499	0.0%	77.8%	11.1%	11.1%	0.0%	0.0%	0.0%	12%
	2,500 to 4,999	0.0%	66.7%	9.5%	9.5%	4.8%	4.8%	4.8%	14%
	5,000 +	4.2%	6.9%	22.2%	20.8%	18.1%	13.9%	13.9%	48%
Total		6.0%	39.1%	17.2%	13.2%	9.3%	7.3%	7.9%	

Table 19: Number of Full Time Information Security Professionals by Total Number of Organizational Employees (Mattord & Whitman, 2015)

Respondents reported had few unfilled or vacant full-time information security positions at the time the survey was taken as shown in Table 20, also by number of employees:
0, 45.1%; 1-5, 35.4%; 6-10, 7.9%; 11-25, 7.9%; 26-50, 1.8%; 51-100, 1.8%

150 responses		**# of unfilled/vacant full-time information security positions**						
		0	1-5	6-10	11-25	26-50	51-100	% of total resp.
# of employees	1 - 49	67%	33%	0%	0%	0%	0%	8%
	50 - 999	59%	33%	4%	4%	0%	0%	18%
	1,000 - 2,499	72%	28%	0%	0%	0%	0%	12%
	2,500 to 4,999	48%	38%	10%	5%	0%	0%	14%
	5,000 +	28%	40%	11%	13%	4%	4%	48%
Total		45%	37%	7%	7%	2%	2%	

Table 20: Number of Unfilled/Vacant Information Security Positions by Total Number of Employees (Mattord & Whitman, 2015)

Turnover was expected to be an issue with information security positions, however, respondents reported very low percentage of turnover in full-time information security positions over the past few years, with the majority reporting no turnover as shown in Table 21:

150 responses		**Average Turnover Rate for Information Security Professionals**							
		0%	1-5%	6-10%	11-25%	26-50%	51-75%	76-100%	% of total resp.
# of employees	1 - 49	75.0%	16.7%	0.0%	0.0%	0.0%	8.3%	0.0%	8%
	50 - 999	44.4%	33.3%	7.4%	7.4%	0.0%	7.4%	0.0%	18%
	1,000 - 2,499	38.9%	22.2%	22.2%	11.1%	5.6%	0.0%	0.0%	12%
	2,500 to 4,999	38.1%	9.5%	23.8%	23.8%	0.0%	0.0%	4.8%	14%
	5,000 or more	13.9%	30.6%	30.6%	20.8%	2.8%	0.0%	1.4%	48%
Total		30.7%	26.0%	22.0%	16.0%	2.0%	2.0%	1.3%	

Table 21: Average Turnover rate for Information Security Professionals By Total # of Employees (Mattord & Whitman, 2015)

Threats to Information Protection

The primary purpose of the survey was to collect and report threats to information protection. The survey asked respondents *"For each of the following please indicate the extent to which you view the item as a current threat to your information assets,"* first from internal sources, as shown in Table 22:

From Employees or Internal Stakeholders	Not a Threat 1	2	3	4	Severe Threat 5	Comp. Rank[1]
Inability/unwillingness to follow established policy	6.6%	17.2%	**33.6%**	26.2%	16.4%	66%
Disclosure due to insufficient training	8.1%	23.6%	**29.3%**	25.2%	13.8%	63%
Unauthorized access or escalation of privileges	4.8%	24.0%	**31.2%**	**31.2%**	8.8%	63%
Unauthorized information collection/data sniffing	6.4%	26.4%	**40.0%**	17.6%	9.6%	60%
Theft of on-site organizational information assets	10.6%	32.5%	**34.1%**	12.2%	10.6%	56%
Theft of mobile/laptop/tablet and related/connected information assets	15.4%	**29.3%**	28.5%	17.9%	8.9%	55%
Intentional damage or destruction of information assets	22.3%	**43.0%**	18.2%	13.2%	3.3%	46%
Theft or misuse of organizationally leased, purchased or developed software	29.6%	**33.6%**	21.6%	10.4%	4.8%	45%
Web site defacement	**43.4%**	33.6%	16.4%	4.9%	1.6%	38%
Blackmail of information release or sales	**43.5%**	37.1%	10.5%	6.5%	2.4%	37%

Table 22: Current Threat to Information Assets from Internal Sources (Mattord & Whitman, 2015)

Then from external sources, as shown in Table 23:

From Outsiders or External Stakeholders	Not a Threat 1	2	3	4	Severe Threat 5	Comp Rank[1]
Unauthorized information collection/data sniffing	6.4%	14.4%	21.6%	**32.8%**	24.8%	71%
Unauthorized access or escalation of privileges	7.4%	14.0%	26.4%	**31.4%**	20.7%	69%
Web site defacement	8.9%	23.6%	22.8%	**26.8%**	17.9%	64%
Intentional damage or destruction of information assets	14.0%	**32.2%**	18.2%	24.8%	10.7%	57%
Theft of mobile/laptop/tablet and related/connected information assets	20.5%	25.4%	**26.2%**	15.6%	12.3%	55%
Theft of on-site organizational information assets	21.1%	24.4%	**25.2%**	17.9%	11.4%	55%
Blackmail of information release or sales	**31.1%**	30.3%	14.8%	14.8%	9.0%	48%
Disclosure due to insufficient training	**34.5%**	21.8%	22.7%	13.4%	7.6%	48%
Inability/unwillingness to follow established policy	**33.6%**	29.4%	18.5%	6.7%	11.8%	47%
Theft or misuse of organizationally leased, purchased or developed software	**31.7%**	30.1%	22.8%	9.8%	5.7%	46%

Table 23: Current Threat to Information Asset from External Sources (Mattord & Whitman, 2015)

[1] Comparative ranking calculated based on the aggregate value of the number of responses for that value times 5 points for a "severe threats" selection, etc. down to 1 point for "not a threat", then converted to a percentage of the maximum possible points.

Respondents were then asked to specify the extent to which a list of items were viewed as threats to information assets. The results are shown in Table 24:

General Threats to Information Assets	Not a Threat 1	2	3	4	Severe Threat 5	Comp Rank[1]
Electronic Phishing/Spoofing attacks	0.8%	13.1%	16.4%	32.0%	**37.7%**	79%
Malware attacks	1.7%	12.4%	27.3%	**36.4%**	22.3%	73%
Unintentional employee/insider mistakes	2.4%	17.1%	26.8%	**35.8%**	17.9%	70%
Loss of trust due to information loss.	4.1%	18.9%	27.0%	22.1%	**27.9%**	70%
Software failures or errors due to unknown vulnerabilities in externally acquired software	5.6%	18.5%	28.2%	**33.9%**	13.7%	66%
Social engineering of employees/insiders based on social media information	8.1%	14.6%	32.5%	**34.1%**	10.6%	65%
Social engineering of employees/insiders based on other published information	8.9%	19.5%	24.4%	**32.5%**	14.6%	65%
Software failures or errors due to poorly developed, internally created, applications.	7.2%	21.6%	24.0%	**32.0%**	15.2%	65%
SQL injections	7.6%	17.6%	**31.9%**	29.4%	13.4%	65%
Social engineering of employees/insiders based on organization's web sites	11.4%	19.5%	23.6%	**31.7%**	13.8%	63%
Denial of Service (and Distributed DoS) attacks	8.2%	23.0%	27.9%	**32.8%**	8.2%	62%
Software failures or errors due to known vulnerabilities in externally acquired software	8.9%	23.6%	26.8%	**35.8%**	4.9%	61%
Outdated organizational software	8.1%	**28.2%**	26.6%	26.6%	10.5%	61%
Loss of trust due to representation as source of phishing/spoofing attack	9.8%	23.8%	**30.3%**	23.0%	13.1%	61%
Loss of trust due to web defacement.	12.4%	30.6%	**31.4%**	19.8%	5.8%	55%
Outdated organizational hardware	17.2%	**34.4%**	32.8%	12.3%	3.3%	50%
Outdated organization data format	18.7%	**35.8%**	26.8%	13.8%	4.9%	50%
Inability/unwillingness to establish effective policy by management	**30.4%**	26.4%	24.0%	13.6%	5.6%	48%
Hardware failures or errors due to aging equipment	19.5%	**39.8%**	24.4%	14.6%	1.6%	48%
Hardware failures or errors due to defective equipment	17.9%	**48.0%**	24.4%	8.1%	1.6%	46%
Deviations in quality of service from other provider	25.2%	**38.7%**	25.2%	7.6%	3.4%	45%
Deviations in quality of service from data communications provider/ISP	26.4%	**39.7%**	23.1%	7.4%	3.3%	44%
Deviations in quality of service from telecommunications communications provider/ISP (if different from data provider)	29.9%	**38.5%**	18.8%	9.4%	3.4%	44%
Loss due to other natural disaster	31.0%	**37.9%**	23.3%	6.9%	0.9%	42%
Loss due to fire	26.2%	**49.2%**	21.3%	3.3%	0.0%	40%
Deviations in quality of service from power provider	36.1%	**43.4%**	12.3%	5.7%	2.5%	39%
Loss due to flood	33.9%	**43.8%**	19.8%	1.7%	0.8%	38%
Loss due to earthquake	**41.7%**	35.8%	15.0%	6.7%	0.8%	38%

Table 24: General Threats to Information Assets (Mattord & Whitman, 2015)

Finally, the respondents were asked the extent to which a series of technologies posed a current source of risk to the security of their information assets, as shown in Table 25:

Technology as a Current Source of Risk	Not a Concern 1	2	3	4	A Severe Concern 5	Comp Rank[1]
Cloud-based data storage	5.0%	13.2%	25.6%	**31.4%**	24.8%	72%
Cloud-based applications	5.0%	16.7%	29.2%	**34.2%**	15.0%	68%
Mobile technologies	3.4%	16.8%	32.8%	**37.8%**	9.2%	67%
"Bring Your Own" Devices (BYOD)	8.3%	16.7%	27.5%	**31.7%**	15.8%	66%
Social media	4.2%	20.0%	**38.3%**	28.3%	9.2%	64%
3rd party payment systems	12.6%	27.7%	**32.8%**	20.2%	6.7%	56%
Open-source applications	8.3%	**34.2%**	**34.2%**	21.7%	1.7%	55%
Big Data repositories	12.5%	30.0%	**32.5%**	21.7%	3.3%	55%
Virtualization technologies	16.7%	**40.0%**	23.3%	16.7%	3.3%	50%
Low-bid contracts	22.2%	**35.9%**	23.1%	12.8%	6.0%	49%

Table 25: Technologies Identified as a Current Sourced of Risk (Mattord & Whitman, 2015)

SUMMARY OF FINDINGS OF THIS STUDY

The study found that the dominant threats that have permeated the literature, both academic and industry/trade press, include Malware and "confidence" attacks on employees (social engineering, phishing, spoofing and pretexting). Even in the current environment of security-focused software development, software issues (failures or errors) remain a concern, as does employee privilege escalation. The low-hanging fruit would seem to be those confidence attacks that could be mitigated through effective security education, training and awareness programs where users are informed on how to look out for fraudulent communications that attempt to conscript them into serving as a function of an attack.

CONCLUSIONS

According to Crossler et. al (2013), additional research is needed in behavioral areas of information security, specifically in areas of "Separating insider deviant behavior from insider misbehavior and Unmasking the mystery of the hacker world" (Crossler et. al, 2013). These topics directly relate to understanding threats from an insiders and outsiders respectively. As General Sun Tzu Wu wrote "If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle" (Wu, n.d.). It is the task of all information security professionals, academics and those managers responsible for the protection of information assets to fully understand and *know* their enemy in order to effective protect their assets in the ongoing campaign against threats to information protection.

REFERENCES

ACSC (2015). Australian Cyber Security Centre "2015 Threat Report." WWW Document viewed 7/15/2016 from www.acsc.gov.au/publications/ACSC_Threat_Report_2015.pdf.

Baracaldo, N. and Joshi, J. (2013). "An adaptive risk management and access control framework to mitigate insider threats." Computers & Security, 1-18. http://dx.doi.org/10.1016/j.cose.2013.08.001

Computer Economics (2009). "Insider Misuse of Computing Resources: Countering Unauthorized Downloading, File Sharing, Instant Messaging, and Other Risks of Employee Abuse." WWW document viewed 7/16/2016 from www.computereconomics.com/page.cfm?name=Insider_Misuse.

Crossler, R., Johnston, A., Lowry, P., Hu, Q., Warkentin, M., and Baskerville, R. (2013). "Future directions for behavioral information security research," Computers & Security, 32, 90-101.

CSI (1999-2011). "Computer Security Institute's Annual Computer Crime and Security Surveys." WWW documents viewed 2000-2012 from www.gocsi.com.

CyberEdge (2016). CyberEdge Group "2016 Cyberthreat Defense Report for North America, Europe, Asia Pacific, and Latin America." WWW Document viewed 7/15/2016 from www.cyber-edge.com/2016-cdr/.

Dell (2016). "Dell Security Annual Threat Report." WWW Document viewed 7/15/2016 from www.sonicwall.com/whitepaper/2016-dell-security-annual-threat-report8107907.

Ernst & Young (2015). "EY's Global Information Security Survey 2015: Creating trust in the digital world." WWW Document viewed 7/15/2016 from www.ey.com/GL/en/Services/Advisory/ey-global-information-security-survey-2015-1.

Harrington, S. (1996). "The Effects of Ethics and Personal Denial of Responsibility on Computer Abuse Judgements and Intentions," MIS Quarterly, 20(3), 257-277.

Hoffer, J. A. and Straub, D. W. (1989) The 9-5 Underground: Are You Policing Computer Crimes? Sloan Management Review. 30, 4 (Summer), 35-43.

Huth, C., Chadwick, D., Claycomb, W. R., and You, I. (2013). "Guest Editorial: A Brief Overview of Data Leakage and Insider Threats," Information Systems Frontiers 15(1), 1-4.

IBM (2016). IBM X-Force® Research "2016 Cyber Security Intelligence Index: Reviewing a Year of serious data breaches, major attacks and new vulnerabilities." WWW Document viewed 7/15/2016 from www-03.ibm.com/security/data-breach/cyber-security-index.html.

InformationWeek (2015). "2015 Strategic Security Survey: The High Cost of Security Breaches." WWW Document viewed 7/10/2016 from http://reports.informationweek.com/abstract/21/12549/Security/2015-Strategic-Security-Survey.html.

ISACA (2016). "State of Security Implications for 2016. An ISACA and RSA Conference Survey." WWW Document viewed 7/10/2016 from www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf.

Jouini, M., Ben Arfa Rabai, L., and Ben Aissa, A. (2014). "Classification of security threats in information systems," 5th International Conference on Ambient Systems, Networks and Technologies. Procedia Computer Science, 32, 489-496.

Kaspersky (2015a). "Consumer Security Risk Survey: From Scared to Aware: Digital Lives in 2015." WWW Document viewed 7/10/2016 from https://press.kaspersky.com/files/2015/08/Kaspersky_Lab_Consumer_Security_Risks_Survey_2015_ENG.pdf.

Kaspersky (2015b). "Global IT Security Risks Survey 2015." WWW Document viewed 7/10/2016 from http://media.kaspersky.com/en/business-security/it-security-risks-survey-2015.pdf

Keller, S., Powell, A., Horstmann, B., Predmore, C., and Crawford, M. (2005). Information Security Threats and Practices in Small Businesses. Information Systems Management, Spring, 7-19.

Kim, S.H. and Kim, B.C. (2014). "Differential Effects of Prior Experience on the Malware Resolution Process," MIS Quarterly, 38(3), 655-678.

Liang, H. and Xue, Y. (2009). "Avoidance of Information Technology Threats: A Theoretical Perspective," MIS Quarterly, 33(1), 71-90.

Loch, K. D., Carr, H. H., and Warkentin, M. E. (1992). "Threats to Information Systems: Today's Reality, Yesterday's Understanding," MIS Quarterly (16), 173-186.

Magklaras, G., and Furnell, S. (2001). "Insider Threat Prediction Tool: Evaluating the Probability of It Misuse," Computers & Security (21:1), 62-73

Mattord, H. and Whitman, M. (2015) "2015 SEC/CISE Threats to Information Protection Report Including a Current Snapshot of the State of the Industry." Security Executive Council. https://www.securityexecutivecouncil.com.

Ponemon (2015a). Ponemon Institute. "2015 Cost of Cyber Crime Study: Global." WWW Document viewed 7/5/2016 from www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/.

Ponemon (2015b). Ponemon Institute. "2015 Global Megatrends in Cybersecurity." WWW Document viewed 7/5/2016 from www.raytheon.com/news/rtnwcm/groups/gallery/documents/content/rtn_233811.pdf.

PwC (2015). PricewaterhouseCoopers. “Key findings from the 2015 US State of Cybercrime Survey.” WWW Document viewed 7/5/2016 from www.pwc.com/us/en/increasing-it-effectiveness/publications/us-cybercrime-survey-2015.html.

Straub, Jr., D. (1990). “Effective IS Security: An Empirical Study”, Information Systems Research 1(3). 255-276.

Straub, D. and Welke, R. (1998) Coping with systems risk: Security planning models for management decision making. MIS Quarterly. 22(4), 441–469.

Sumner, M. (2009). Information Security Threats, A Comparative Analysis of Impact, Probability, and Preparedness. Information Systems Management, 26: 2-12.

Verizon (2016). “Verizon’s 2016 Data Breach Investigations Report.” WWW Document viewed 7/17/2016 from www.verizonenterprise.com/verizon-insights-lab/dbir/2016/.

Wang, J., Chaudhury, A., and Rao, H. (2008). “A Value-at-Risk Approach to Information Security Investment,” Information Systems Research 19(1), 106-120.

Wang, J., Gupta, M and Rao, R. (2015). “Insider Threats in a Financial Institution: Analysis of Attack-Proneness of Information Systems Applications”. MIS Quarterly, 39(1), 91-112.

Warkentin, M., and Willison, R. (2009). “Behavioral and Policy Issues in Information Systems Security: The Insider Threat,” European Journal of Information Systems (18), 101-105.

Whitman, M., & Mattord, H. (2012). Threats to Information Security Revisited. Journal of Information Systems Security, 8(1), 21-41.

Whitman, M. and Mattord, H., (2016). Management of Information Security, 5th edition. Cengage/Course Technology.

Willison, R., and Warkentin, M. (2013). “Beyond Deterrence: An Expanded View of Employee Computer Abuse,” MIS Quarterly, 37(1), 1-20.

Winkler, I., (2006). “Time to End the FBI/CSI Study?” Computerworld Online. WWW Document viewed June 26, 2016 from http://www.computerworld.com/article/2546917/security0/time-to-end-the-fbi-csi-study-.html.

Wu, Sun Tzu. (n.d.) Art of War. WWW document viewed 8/12/2016 from http://classics.mit.edu/Tzu/artwar.html.